UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/558,848	09/28/2006	James F. Riordan	CH920030006US1	7159

54856 7590 08/20/2008

LOUIS PAUL HERZBERG
3 CLOVERDALE LANE
MONSEY, NY 10952

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
08/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/558,848	RIORDAN, JAMES F.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/20/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action in response to application September 28, 2006. Claims (1) is pending.

Priority

2. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) - (d) is acknowledged.

The application is filed on September 28, 2006 but is a 371 case of PCT/IBO3/05328 application filed 11/20/2003 and has a foreign priority to European Patent Office (EPO) 03405393.4 filed on 05/30/2003.

.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over by Copeland (US Patent No. 7,290,283) in view of Ricciulli (US Patent No. 6,473,405).

4. As to claim 1, Copeland teaches a **method for detecting attacks on a data communications network having a plurality of addresses for**

assignment to data processing systems in the network [abstract], **the method comprising:**

identifying data traffic on the network originating at any assigned address and addressed to any unassigned address (i.e., ...teaches a port profiling system detects unauthorized network usage. ... further teaches port profiling system analyzes network communications to determine the service ports being used [abstract, lines 1-4]), **said unassigned address is an address which is free and not assigned to user systems** (i.e., ... teaches a system collects flow data from packet headers between two hosts or Internet Protocol (IP) addresses [abstract, lines 5-8] ... further teaches (i.e., ... teaches a determination is made whether monitored flow is a valid connection with data flow [col. 3, lines 60-67]);

inspecting any data traffic so identified for data indicative of an attack (i.e., ... teaches collected flow data is analyzed to determine the associated network service provided. ... teaches a host data structure is maintained containing a profile of the network services normally associated with the host [abstract])

and, on detection of data indicative of an attack , generating an alert signal (i.e., ... teaches if the observed network service is not one of the normal network services performed as defined by the port profile for that host, an alarm signal is generated and action can be taken based upon the detection of an Out of Profile network service [abstract]), **where the step of inspecting comprises spoofing replies to requests contained in the data traffic identified** (i.e., ...

teaches the port profiling engine works by assigning data packets to various legitimate flows. ... teaches a legitimate flow is a communication in which data is sent and acknowledged. ... teaches a port scans and some other illegitimate flows typically do not send data with the packets [col. 7, lines 55-67]);

on generation of the alert signal (i.e., ... teaches if the observed network service is not one of the normal network services performed as defined by the port profile for that host, an alarm signal is generated and action can be taken based upon the detection of an Out of Profile network service [abstract]),

rerouting any data traffic originating at the address assigned to the data processing system originating the data indicative of the attack to a disinfection address on the network (i.e., ...teaches router technology [claim 32] Those skilled in the art would recognize rerouting is inherent functionality of a router. ... furthermore Copeland teaches a messages can also be sent to cause automated devices such as a firewall manager to drop (e.g., reroute) packets going to or from an offending host [col. 28, lines 1-5]).;

on generation of the alert signal, sending an alert message to the disinfection address(i.e., ... teaches a messages can also be sent to cause automated devices such as a firewall manager to drop packets going to or from an offending host [col. 28, lines 1-5]);

where the alert message comprises data indicative of the attack detected on receipt of the alert message, sending a warning message from the disinfection address to the address assigned to the data processing system originating the data indicative of the attack(i.e., ... teaches if the

observed network service is not one of the normal network services performed as defined by the port profile for that host, an alarm signal is generated and action can be taken based upon the detection of an Out of Profile network service [abstract].;

including in the warning message program code for eliminating the attack when executed by the data processing system originating the data indicative of the attack (i.e., ... teaches if the observed network service is not one of the normal network services performed as defined by the port profile for that host, an alarm signal is generated and action can be taken based upon the detection of an Out of Profile network service [abstract] ... further teaches (i.e., ... teaches a messages can also be sent to cause automated devices such as a firewall manager to drop packets going to or from an offending host [col. 28, lines 1-5]);

supporting an entity in the handling of the detected attack by one of providing instructions for use of, assistance in executing, and execution of disinfection program code [fig. 2];

providing a report to said entity containing information related to one of alert, disinfection, rerouting, logging, discarding of data traffic in the context of a detected attack (i.e., ... teaches numerous other queries and reports can be generated for review and analysis by a network system administrator [col. 27, lines 45-52]);

providing said steps of identifying, inspecting and generating to a plurality of entities and using technical data derived from the attack-

handling for one of said entities for the attack-handling for another of said entities, wherein the alert message comprises data indicative of the attack detected (i.e., ... teaches It analyzes certain statistical data and tracks the associated network services. ... teaches a engine compares recent activity to a predetermined port profile. ... teaches an alarm is generated when a host uses a service that is not in its port profile [col. 14, lines 10-20]).

However Copeland does not expressly teach:

billing said entity for the execution of at least one of the steps of this method, the charge being billed determined in dependence of one of the size of the network, the number of unassigned addresses monitored, the number of assigned addresses monitored, the volume of data traffic inspected, the number of attacks identified, the number of alerts generated, the signature of the identified attack, the volume of rerouted data traffic, the degree of network security achieved, the turnover of said entity,

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Copeland as introduced by Ricciulli. Ricciulli discloses:

billing said entity for the execution of at least one of the steps of this method, the charge being billed determined in dependence of one of the size of the network, the number of unassigned addresses monitored, the

number of assigned addresses monitored, the volume of data traffic inspected, the number of attacks identified, the number of alerts generated, the signature of the identified attack, the volume of rerouted data traffic, the degree of network security achieved, the turnover of said entity, and (for purposes of billing for security relative and network traffic routing function Ricciulli provides the capability to provide cost analysis for pertinent security and network traffic control functions as prescribed by Copeland [Ricciulli; abstract]. Both Copeland and Ricciulli provides robust and scalable systems as such warranting the desirability to combine Copeland and Ricciulli to provide billing for the execution of process steps relative to security and network traffic control).

Therefore, given the teachings of Ricciulli, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Copeland by employing the well known features of network security and traffic control cost determination disclosed above by Ricciulli, for which network security and traffic control will be enhanced [Ricciulli; abstract].

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is

(571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131